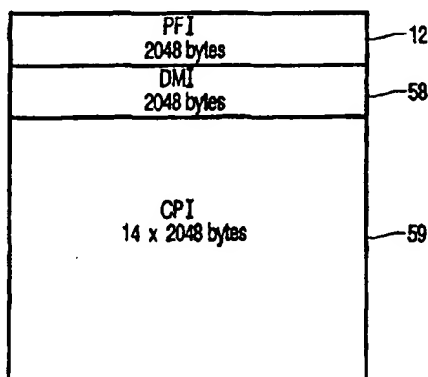




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : G11B 20/00, 20/12, 7/007		(11) International Publication Number: WO 00/21085
A1		(43) International Publication Date: 13 April 2000 (13.04.00)
(21) International Application Number: PCT/EP99/06789 (22) International Filing Date: 14 September 1999 (14.09.99) (30) Priority Data: 98203340.9 5 October 1998 (05.10.98) EP (71) Applicant: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL). (72) Inventors: KAMPERMAN, Franciscus, L., A., J.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). STARING, Antonius, A., M.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). (74) Agent: FAESSEN, Louis, M., H.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published With international search report.

(54) Title: SYSTEM FOR COPY PROTECTION OF RECORDED INFORMATION



(57) Abstract

An information carrier, e.g. an optical disc, comprises information arranged according to a recording format. The information includes format information indicative of parameters of the recording format such as start and stop addresses of user information. The information is recorded according to predefined encoding rules, which correspond to rules of a different recording format, e.g. CD-ROM or DVD, that prescribes a predefined location (12) on the information carrier for recording the format information. However the predefined location (12) comprises a confusion pattern (CON) and the format information is recorded at a second location (CPS1) different from the predefined location. A non-compliant player is unable to read or copy the information carrier because the reading is disturbed by the wrong parameters of the recording format. According to the invention a recorder is arranged for recording said confusion pattern and relocating said format information, whereas a player is arranged to retrieve the relocated format information.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

System for copy protection of recorded information.

The invention relates to an information carrier comprising information arranged according to a recording format, the information being recorded according to predefined encoding rules and including format information indicative of parameters of the recording format.

5 The invention further relates to a player for reproducing information from the information carrier, the player comprising format means for providing parameters of the recording format, and reading means for retrieving the information in dependence on the parameters of the recording format.

10 The invention further relates to a recorder for recording information arranged according to a recording format on an information carrier, the recorder comprising recording means for recording the information according to predefined encoding rules and for including format information indicative of parameters of the recording format.

15 The invention further relates to a method for recording information arranged according to a recording format on an information carrier, in which method the information is recorded according to predefined encoding rules, and format information is included indicative of parameters of the recording format.

20 A system for copy protection of recorded information comprising an information carrier, a player and a recorder, is known from US 5737286 (D1 of the list of relevant documents). Copy protection may comprise preventing the creation of a digital copy on a different carrier, allowing some copy activity (e.g. only a first generation of copies), or controlling, verifying or restricting the access to protected information. The information carrier comprises information recorded according to an existing recording format, e.g. the CD-
25 ROM format. The format prescribes the structure of recorded information, such as what type of information is recorded at which location on the disc, e.g. that the recorded area starts with a lead-in area at a predetermined diameter. Such a format may also include other parameters such as a type of recording layer (recordable, pre-recorded, etc), a number of recording layers and physical parameters of the recording process (density, reflectivity, etc). Format

information, which gives actual values of parameters of the recording format used on an information carrier in question, is included in the recorded information on said record carrier, and is intended for use by the player when reproducing user information from said information carrier, e.g. format parameters in sector headers or a Table Of Contents (TOC) which
5 comprises information on where the user information starts and ends. The information on the information carrier is recorded according to predefined encoding rules, such as the channel code (EFM) for translating the user bytes into lengths of optically readable pits in the CD, and error coding and sector structuring rules. Such encoding rules are usually a predefined part of the recording format, and are not indicated in the format information recorded on the disc. The
10 player for reproducing the information carrier comprises reading means for reading and decoding the recorded information according to the inverse of said encoding rules.

In the system of D1 the player and information carrier form a system for controlled information reproduction, in which reproduction of illegally copied information is counteracted. Copy protection has a long history in audio or video publishing. The presently
15 installed base of equipment, in particular Personal Computers (PC) with audio/video cards, provide little protection against unauthorized copying. In any copy-protection scheme, the most difficult issue is that a pirate can always attempt to playback an original disc, treat the content as if it were an analog home recording and record this. However the best quality is only available when a digital copy can be made. For digital storage media such as Digital
20 Compact Cassette (DCC), "copy bits" have been defined, which bits indicate a copyright status, e.g. "no copy allowed", "free copy" or "one generation of copy allowed". Other copy bits may indicate that the medium storing the information must be a "professional" medium manufactured by pressing and not a "recordable" disc. However such copy bits can easily be ignored by the pirate, e.g. using a PC as copy engine. Devices which do not obey the rules of a
25 format are called 'non-compliant' devices.

The copy protection of the system known from D1 is based on a so-called medium mark, i.e. a physical mark representing a bitpattern indicating the copyright status of the medium, e.g. a "professional" disk manufactured by pressing. The medium mark itself is not copyable or changeable by standard recording equipment and said bitpattern is to be
30 verified by the compliant player and may even be required for reproduction, e.g. a descramble code for recovering information stored as scrambled information. On the record carrier of D1 information is recorded in the track in a predefined manner represented by optically readable patterns formed by variation of a first physical parameter, such as the height of the scanned surface. The medium mark is constituted by a variations of a second parameter of the track

which are modulated according to said bitpattern, e.g. an excursion in a transverse direction of the track formed by a pregroove, also denoted as wobble. If the information of the known record carrier is copied "bit-by-bit" by a pirate on a writable information carrier using a non-compliant device, the information of this copy cannot be reproduced by a compliant player, because the copy does not comprise the medium mark corresponding to the illegally copied information. However detecting the medium mark and retrieving said bitpattern requires additional elements in the compliant player, whereas a compliant recorder preferably also detects any medium mark on a recordable disc. Hence, the known system for copy protection requires expensive and complex players and recorders.

It is an object of the invention to provide a system in which accessing and copying recorded information is controlled and which is less complex.

For this purpose, the information carrier as described in the opening paragraph is characterized in that, while said encoding rules correspond to rules of a different recording format that prescribes a predefined location on the information carrier for recording the format information, the predefined location comprises a confusion pattern and in that the format information is recorded at a second location different from the predefined location. The player as described in the opening paragraph is characterized in that the format means are arranged for detecting the recording format of the information carrier, and in that the format means are arranged for supplying predefined parameters or for retrieving the format information from the second location when said recording format is detected. The recorder as described in the opening paragraph is characterized in that the recording means are arranged for recording a confusion pattern at the predefined location and for recording the format information at a second location different from the predefined location.

Existing, non-compliant read devices will try to read the format information from said predefined location, but will read the confusion pattern instead. This confusion pattern will cause the existing devices to stop reading, or to use wrong settings for the reading means, which causes the reading process to malfunction. This has the effect, that existing devices are prevented from accessing copy protected audio/video information from the information carrier, because they cannot read the format information. Hence a digital copy cannot be made using non-compliant players or recorders, even if they are not aware of (or manipulated to

disregard) any copy protection information bits. While the format information is hidden for existing players, it can be easily retrieved by the player according to the invention. This has the advantage, that the reading means, although comprising complex decoding and error correction circuits, can be manufactured relatively cheap because substantially all components are common to existing players.

The invention is based on the recognition, that the format information must be available, but cannot be manipulated in non-compliant devices. By relocating the format information uncontrolled playback of copy protected discs by existing, non compliant devices, can be prevented. In particular, the reading and/or recording of format information cannot be controlled or manipulated by a pirate, because such steps are usually built in a control unit in the basic read or write engine. As an alternative to relocating the format information, it would be possible to change the predefined encoding rules of an existing recording system for copy protection purposes. This however increases the cost of a new copy protected recording system, because complex IC's must be redesigned and produced specifically for the new players and recorders. So in practice the encoding rules must be equal to the encoding rules of an existing system, e.g. the Compact Disc (CD) or Digital Versatile Disc (DVD) system, and non-compliant devices comprising such encoding and decoding means are available. A record carrier recorded with said encoding rules could be played back on a non-compliant device, e.g. on the PC, and manipulation of audio/video information would be possible. However by relocating the format information according to the invention, non-compliant players are prevented from uncontrolled playback, because they rely on the format information, such as the TOC in CD or Physical Format information in DVD, for accessing the audio/video information.

A preferred embodiment of the system is characterized in that the second location is variably selected within a predefined area of the information carrier and/or in that the format information located at said second location is encrypted using an encryption key. Variably selected means that when an audio/video production is put on a master disc for mass reproduction, a specific second location for that production is selected randomly from the range of possible locations. Alternatively or in combination one encryption key is generated randomly for each new production. This has the advantage, that it is more difficult for a pirate to locate or retrieve the correct format information.

Further advantageous, preferred embodiments according to the invention are given in the dependent claims.

These and other aspects of the invention will be apparent from and elucidated further with reference to the embodiments described by way of example in the following description and with reference to the accompanying drawings, in which

- 5 Figure 1 shows a record carrier,
 Figure 2 shows a logical sector structure,
 Figure 3 shows a map of control information of an existing format,
 Figure 4 shows format information in a predefined structure,
 Figure 5 shows a confusion pattern,
10 Figure 6 shows a map of control information including copy control
 information,
 Figure 7 shows disc format data,
 Figure 8 shows key information,
 Figure 9 shows a playback apparatus,
15 Figure 10 shows a recording device,
 Figure 11 shows an encryption process, and
 Figure 12 shows a decryption process.

Corresponding elements in different Figures have identical reference numerals.

20

Figure 1a shows a disc-shaped information carrier 11 having a track 19 and a central hole 10. The track 19 is arranged in accordance with a spiral pattern of turns constituting substantially parallel tracks on an information layer. The information carrier may be an optical record carrier, e.g. an optical disc, having an information layer of a recordable type or of a prerecorded type. The record carrier is intended for carrying user information, for
25 example audio or video or computer programs. Examples of a recordable disc are the CD-R and CD-RW, and the DVD-RAM, whereas the audio CD is an example of a prerecorded disc. The prerecorded type can be manufactured in a well known way by first recording a production of audio or video content on a master disc and subsequently pressing consumer
30 discs. The track 19 on the recordable type of record carrier is indicated by a pre-embossed track structure provided during manufacture of the blank record carrier. The track structure is constituted, for example, by a pregroove 14 which enables a read/write head to follow the track 19 during scanning. The information is represented on the information layer by optically detectable marks recorded along the track, e.g. pits and lands.

Figure 1b is a cross-section taken along the line b-b of the record carrier 11 of the recordable type, in which a transparent substrate 15 is provided with a recording layer 16 and a protective layer 17. The pregroove 14 may be implemented as an indentation or an elevation, or as a material property deviating from its surroundings.

5 The record carrier comprises information recorded according to a recording format. The recording format prescribes the way information is recorded, encoded and logically mapped. The way of recording information in the format includes parameters of the recorded information, e.g. the type and number of recording layers, data speed, etc. Further the format includes encoding rules, such as channel coding, error coding or sector structuring
10 rules. An example of a sector structure is given in Figure 2. The encoding rules of the information carrier according to the invention correspond to known encoding rules, such as the CD or DVD format. The logical mapping may comprise a subdivision of the recordable area in a lead-in, a user data area and a lead-out, and control information for retrieving the user information, such as a Table Of Contents or a file system, e.g. ISO 9660 for CD-ROM.
15 Figures 3 and 4 show examples of such control information, which is mapped on a predefined location on the record carrier, usually in or directly after the lead-in area. Some parameters of the format may vary for different information carriers, and for that reason format information giving the actual values of such parameters is recorded on the information carrier. The encoding rules are necessarily a predefined part of the format, because they have to be known
20 in advance to read and decode any information, and hence the encoding rules are usually not included in the format information. The format information is recorded on a predefined location 12 on the record carrier, because all players need to retrieve said format information before further information can be read.

Figure 2 shows a logical sector structure, as an example of a predefined
25 encoding rule. The first part 51,52,53 constitutes a header. The first 4 bytes 51 constitute Identification Data (ID), e.g. a sector number and sector type information. The next 2 bytes 52 are for ID Error Detection (IED), and the 6 bytes 53 are Reserved (RSV) for further use, which may include copy protection status bits. After the header 12 rows 54 of main data follow (the first row being 160 bytes, then ten rows of 172 bytes and the last row of 168 bytes, 2048 bytes
30 in total). At the end a 4 bytes Error Detection code (EDC) 55 is added.

Figure 3 shows a schematic map of control information in the first part of the recorded area of an information carrier according to an existing format. Usually optical information carriers are logically mapped and recorded/read in outward direction, starting at a predefined diameter at the inner side of the pattern of tracks 13. The first section of the map

contains format information, called Physical Format Information (PFI), and constitutes the predefined location 12. The second section 58 comprises Disc Manufacturing Information (DMI), and the third section 59 comprises Content Provider Information, which is further information about the user data, e.g. audio/video production information, recorded in the user information area. This control information may be recorded repeatedly for protection against read errors and dust or scratches. The map given in Figure 3 is an example, as a control information structure may comprise other elements or may have a different set-up, but according to the existing format the control information structure should comprises at least some format information at some predefined location 12.

Figure 4 shows format information in a predefined structure. The structure and type of parameters included are predefined in the format, because all player or recorder devices must be able to retrieve the value of said parameters for controlling the reading and/or recording means. The first parameter gives the Disc Category and Version (DCV), for example read-only and according to specification version number 1. Then the next parameter gives the Disc Size and transfer Rate (DSR). The third parameter gives the Disc Structure (DS), for example the number of layers and the track layout. The fourth parameter gives the Recording Density (RD), and the fifth parameter the Data Zone (DZ), for example the first and last physical sector address of the user data area. Further bytes 16, 17-31 and 32-2047 are reserved (RSV) for further use. The information carrier according to the invention complies with the encoding rules of an existing format, but the format information is relocated from the predefined location to a different location. The different location may be somewhere else within a map corresponding to Figure 3, for example in the CPI area 59 as shown in Figure 6, or in the reserved area bytes 16-2047 shown in Figure 4. The predefined location 12 comprises a confusion pattern, which gives wrong values to the parameters of the format. A device for playing information carriers of the existing format, a so-called non-compliant device, will read the confusion pattern, and the reading of further information will be prevented because the wrong format parameters cause wrong settings in the non-compliant device or the reading process is aborted by the control program of the non-compliant device.

In an embodiment of the information carrier according to the invention the format information comprises user key information for processing the user information. As the format information is relocated as indicated above, and because the user key information is required to process the user information, a pirate player cannot fully retrieve the user information even if it manages to read information from the user area. The processing may comprise decryption of user audio or video information, or access control to certain options

within a computer program, or verification or transfer of a copy control status. In an embodiment only part of the user information is encrypted. For example decryption is required only for some sectors of the user information area as indicated by a bit in the reserved bytes (RSV) 53 in the sector structure shown in Figure 2. When only one sector is encrypted out of every few (e.g. 2 to 10) this has the advantage that less time is required for decryption and less computing power is required in the player. In a further embodiment the user key information is used for verifying and controlling the copyright status of the user information, and/or for verifying a watermark embedded in the user information. Such user key information, also called a control ticket, is described in D3. The control ticket is used for transferring copy status information and for performing copy generation control in a compliant recorder and/or player as described in D3. Alternatively the control ticket may be encrypted using the user key information and stored at a different location on the information carrier.

Figure 5 shows a confusion pattern in the same structure as the format information of the existing format as shown in Figure 4. The confusion pattern (CON) covers the bytes 0 to 15, which are used in the existing structure of Figure 4. The confusion pattern may be all zero's, or a random pattern. In an embodiment of the information carrier the confusion pattern comprises fake address information in the Data Zone bytes of the existing structure. The fake address information is indicative of an area different from the user information area, e.g. a very short area within the lead-in area or a very large area outside the physical limits of the record carrier. In an embodiment of the record carrier the fake address information is indicative of an area comprising information recorded according to said existing recording format. The confusion pattern in this embodiment comprises valid information, which however only covers that part of the disc which is recorded fully according to the existing format, forming a combination disc. The part according to the existing format may contain a warning message, or alternatively a different representation or a selection (a preview) of the information in the 'copy-protected' area recorded according to the format of the invention. Preferably the 'copy-protected' area does not immediately follow the existing format area, as some drives may ignore the control information and continue playing. Some dummy information or an un-recorded area could be located between said two areas.

Figure 6 shows a schematic map of control information including copy control information. The predefined location 12 comprises the confusion pattern CON instead of the format information PFI. Next, corresponding to the existing format shown in Figure 3, the DMI section 58 and CPI section 59 follow, which CPI section comprises at least one Copy Protection System (CPS) location for recording copy protection system information, e.g. the

relocated format information. In the Figure the CPI section 59 is subdivided in X,Y and Z parts by a first Copy Protection System (CPS1) section 61 and a second Copy Protection System (CPS2) section 62. CPS1 and/or CPS2 comprise the format information. In an embodiment of the information carrier the CPS location is variably selected within a predefined area of the information carrier. In Figure 6 the predefined area is constituted by the CPI area, but any area may be assigned for this purpose in the format according to the invention. The size of parts X,Y and Z varies with the selected CPS location(s), and may even be zero.

In an embodiment the information carrier comprises access information. The access information is indicative of the CPS location of the format information. A pointer to the CPS location may be included in the confusion pattern or the reserved bytes 16-2047 in Figure 4 following the bytes assigned to parameters of the existing format.

In an embodiment the access information includes Copy Protection System Index information (CPSI), which indicates that CPS locations are present and a confusion pattern is recorded in the predefined location. The CPSI comprises a pointer value for searching the relocated format information in the CPS locations is included in the six reserved bytes 53 in the sector structure shown in Figure 2. The CPSI is recorded at some predefined address(es), e.g. in some or all sectors of the lead-in area. Said pointer value may be a relative pointer to a sector number within the control data area shown in Figure 6. When several CPS locations are used, also several pointers may be used in CPSI, or a fixed distance between the CPS locations may be used, or further pointers may be included in the first CPS location.

Figure 7 shows Disc Format Data (DFD), which is format information as relocated to a Copy Protection System location. The first 16 bytes of the DFD information can be structured as given in Figure 4. In an embodiment the information carrier the DFD information located at said second location is encrypted using an encryption key. The encryption key may be fixed and known to compliant devices only. In an embodiment the key information is recorded on the record carrier.

Figure 8 shows key information as recorded in a CPS location. The information carrier comprises the key information for decrypting said encrypted DFD information. The first bytes 0-m comprise a Disc Format Key (DFK), and the next bytes m to n comprise an Encrypted initialisation Vector E_IV. An embodiment of the encryption and decryption process is described with Figures 11 and 12.

Figure 9 shows a playback apparatus according to the invention for reading a record carrier 11, which record carrier is identical to the record carrier shown in Figure 1. The

device is provided with drive means 21 for rotating the record carrier 1, and a read head 22 for scanning the track on the record carrier. The apparatus is provided with positioning means 25 for coarsely positioning the read head 22 in the radial direction on the track. The read head comprises an optical system of a known type for generating a radiation beam 24 guided through optical elements focused to a radiation spot 23 on a track of the information layer of the record carrier. The radiation beam 24 is generated by a radiation source, e.g. a laser diode. The read head further comprises a focusing actuator for moving the focus of the radiation beam 24 along the optical axis of said beam and a tracking actuator for fine positioning of the spot 23 in a radial direction on the centre of the track. The tracking actuator may comprise coils for radially moving an optical element or may be arranged for changing the angle of a reflecting element. The radiation reflected by the information layer is detected by a detector of a usual type, e.g. a four-quadrant diode, in the read head 22 for generating a read signal and further detector signals including a tracking error and a focusing error signal coupled to said tracking and focusing actuators. The read signal is processed by a reading means 27 to retrieve the information in dependence on the parameters of the recording format. The reading means are of a usual type for example comprising a channel decoder and an error corrector which decode the read signal encoded according to the encoding rules prescribed by the format. The retrieved data is passed to a data selection means 28. The data selection means selects user data from all data read and passes the user data to data to output unit 29, which may comprise a data buffer or user data processing means, such as audio or video decompression. The device is further provided with a control unit 20 for receiving commands from a user or from a host computer for controlling the apparatus via control lines 26, e.g. a system bus, connected to the drive means 21, the positioning means 25, the reading means 27 and the data selection means 28, and output unit 29. To this end, the control unit 20 comprises control circuitry, for example a microprocessor, a program memory and control gates, for performing several procedures and functions as described below. The control unit 20 may also be implemented as a state machine in logic circuits. Selection means 28 also retrieves control information from the record carrier, which is passed on to the control unit 20. Control information from the sector structure may be retrieved by reading means 27 while decoding the read signal, e.g. the CPSI information described above.

The control unit 20 comprises format means for providing said parameters of the recording format by retrieving the format information from the CPS location. The CPS location may be known to a compliant device, and in that event the format information can be read immediately. Alternatively a set of parameter values may be predefined and stored in

control unit 20, and said stored parameter values are supplied when said format information is not retrievable from said predefined location. In an embodiment the player comprises detection means for detecting the retrievability of the format information from said predefined location by detecting the confusion pattern and/or the access information. The control unit
5 embodies said detection means, which first read the predefined location, and based on the information read determine if the information carrier is recorded according to the existing format. If the information read is the confusion pattern, this is detected from recognizable wrong values for certain parameters, e.g. all zero's or a too large area for user data. The record carrier may comprise access information, which explicitly indicates the recording format
10 according to the invention, such as a bit in the sector header (see Figure 2). In an embodiment the detection means are arranged to read said access information, in particular the pointer values or CPSI as described above. In an embodiment of the player the format means are arranged for retrieving the format information from the CPS location in dependence on the access information. In the event that the information carrier comprises encrypted format
15 information, the format means are arranged for decrypting the format information. The decryption process is described below with reference to Figure 12. The necessary key information may be read from the information carrier and/or may be stored in the player.

Figure 10 shows a recording device for writing information on a record carrier
11 according to the invention of a type which is (re)writable. A similar device or recording method is used for producing a master disc for manufacturing pressed discs. During the
20 writing operation, marks representing the information are formed on the record carrier. The marks may be in any optically readable form, e.g. in the form of areas with a reflection coefficient different from their surroundings, obtained when recording in materials such as dye, alloy or phase change material, or in the form of areas with a direction of magnetization
25 different from their surroundings, obtained when recording in magneto-optical material. Writing and reading of information for recording on optical disks and usable formatting, error correcting and channel coding rules are well-known in the art, e.g. from the CD system. The marks can be formed by means of a spot 23 generated on the recording layer via a beam 24 of electromagnetic radiation, usually from a laser diode. The recording device comprises similar
30 basic elements as the apparatus for reading described above with Figure 9, i.e. a control unit 20, a drive means 21 and a positioning means 25, but it has a write head 39. User information is presented on the input unit 36, which may comprise of compression means for audio or video. Suitable compression means are described in D2. From the input unit 36 the data is passed to data combination means 37 for adding control data including said format

information. The total data stream to be recorded is passed to writing means 38. The write head 39 is coupled to the writing means 38, which comprise for example a formatter, an error coder and a channel coder. The data presented to the input of the writing means 38 is distributed over logical and physical sectors according to said predefined encoding rules and converted into a write signal for the write head 39. The control unit 20 is arranged for controlling the input unit 36, the data combination means 37 and the writing means 38 via control lines 26 and for performing the positioning procedure as described above for the reading apparatus. Usually the recording apparatus will also be arranged for reading having the features of the playback apparatus and a combined write/read head. The recorder also comprises means for including format information indicative of parameters of the recording format.

According to the invention the control unit 20 of the recording device is arranged for recording a confusion pattern at the predefined location and recording the format information at a CPS location different from the predefined location. In further embodiments of the recording device the control unit 20 is arranged for recording the format, access or key information as defined above for the information carrier with reference to Figures 5 to 8 and as defined in the claims for the information carrier. A method of recording for producing an information carrier is arranged to perform the functions of recording the format, access or key information as defined above for the recorder.

Figure 11 shows an encryption process. The encryption process is performed in an embodiment of the control unit 20 of the recorder shown in Figure 10. The encryption is used for encrypting the format information to encrypted DFD bytes as discussed above with reference to Figures 7 and 8. Any suitable encryption algorithm can be used, for example as described in D4, in particular on page 390-392 in chapter 16.9 Additive Generators. Such an algorithm can be used to produce random words. The algorithm shown processes 4 bytes in one cycle. In a first step 71 an Encrypted Initialisation Vector (E_IV) is generated using key DFK and starting from a random number IV added to a predefined constant C in adder step 70. The resulting E_IV is recorded on the information carrier. The E_IV is added to byte 0-3 of plain format information in adder step 72, and processed in encryption step 73 using the starting key values from the first step 71. Now the bytes 0-3 of the encrypted DFD are available. This step is repeated 4 times up to last step 75 for last bytes 12-15 of DFD. The 16 bytes encrypted DFD are recorded on the information carrier.

Figure 12 shows a decryption process complementary to the encryption process shown in Figure 11. The decryption process is performed in an embodiment of control unit 20

of the player. In a first step 81 the E_IV is decrypted using DFK as key info. The resulting IV is not used directly, but the decryption process is initialised for the next cycle. In the next cycle in a next decryption step 83 the bytes 0-3 of encrypted DFD are decrypted and added to E_IV in an adder step 82 to result in plain format information bytes 0-3. The cycle is repeated to last bytes 12-15 of encrypted DFD are decrypted in decryption step 85 and added to the previous result in adder step 84 to result in plain bytes 12-15 of format information.

Although the invention has been explained by embodiments using audio or video, the invention can be applied also to computer data. In the embodiments the information carrier is embodied by an optical disc, but any other carrier can be used in the invention, such as tape or broadcast, as long as format information is supplied on the carrier corresponding to an existing format prescribing a predefined way which cannot be easily manipulated. Further, the invention lies in each and every novel feature or combination of features described above.

List of related documents

- (D1) US 5,737,286 (PHN 13922)
Closed information system with physical copy protection
- 5 (D2) WO 98/16014-A1 (PHN 16452)
1 bit ADC and lossless compression of audio
- (D3) WO 98/33325-A2 (PHN 16372)
Copy protection system based on watermarking and control ticket.
- (D4) Applied cryptography, by Bruce Schneider
10 ISBN 0-471-12845-7

CLAIMS:

1. Information carrier comprising information arranged according to a recording format, the information being recorded according to predefined encoding rules and including format information indicative of parameters of the recording format, characterized in that, while said encoding rules correspond to rules of a different recording format that prescribes a predefined location on the information carrier for recording the format information, the predefined location comprises a confusion pattern and in that the format information is recorded at a second location different from the predefined location.
2. Information carrier as claimed in claim 1, characterized in that the second location is variably selected within a predefined area of the information carrier.
3. Information carrier as claimed in claim 1 or 2, characterized in that the information carrier comprises access information indicative of the location of the format information.
4. Information carrier as claimed in claim 1, 2 or 3, characterized in that the format information located at said second location is encrypted using an encryption key.
5. Information carrier as claimed in claim 4, characterized in that the information carrier comprises key information for decrypting said encrypted information.
6. Information carrier as claimed in any of the claims 1 to 5, characterized in that, while the format information comprises address information indicative of a user information area, the confusion pattern comprises fake address information indicative of an area different from the user information area.
7. Information carrier as claimed in claims 6, characterized in that the fake address information is indicative of an area comprising information recorded according to said different recording format.

8. Information carrier as claimed in any of the claims 1 to 7, characterized in that the format information comprises user key information for processing user information.

5 9. Player for reproducing information from the information carrier claimed in any of the claims 1 to 8, the player comprising format means for providing parameters of the recording format, and reading means for retrieving the information in dependence on the parameters of the recording format, characterized in that the format means are arranged for detecting the recording format of the information carrier, and in that the format means are
10 arranged for supplying predefined parameters or for retrieving the format information from the second location when said recording format is detected.

10. Player as claimed in claim 9, characterized in that format means are arranged for detecting the recording format by detecting the confusion pattern from said predefined
15 location and/or the access information.

11. Player as claimed in claim 9 or 10 for reproducing information from the information carrier claimed in any of the claims 3 to 8, characterized in that the format means are arranged for retrieving the format information from the second location in dependence on
20 the access information and/or the key information.

12. Recorder for recording information arranged according to a recording format on an information carrier, the recorder comprising recording means for recording the information according to predefined encoding rules and for including format information indicative of
25 parameters of the recording format, characterized in that, while said encoding rules correspond to rules of a different recording format that prescribes a predefined location on the information carrier for recording the format information, the recording means are arranged for recording a confusion pattern at the predefined location and for recording the format information at a second location different
30 from the predefined location.

13. Method for recording information arranged according to a recording format on an information carrier, in which method the information is recorded according to predefined

- encoding rules, and format information is included indicative of parameters of the recording format,
- characterized in that, while said encoding rules correspond to rules of a different recording format that prescribes a predefined location on the information carrier for recording the format information, the method comprises recording a confusion pattern at the predefined location
- 5 and recording the format information at a second location different from the predefined location.

1/5

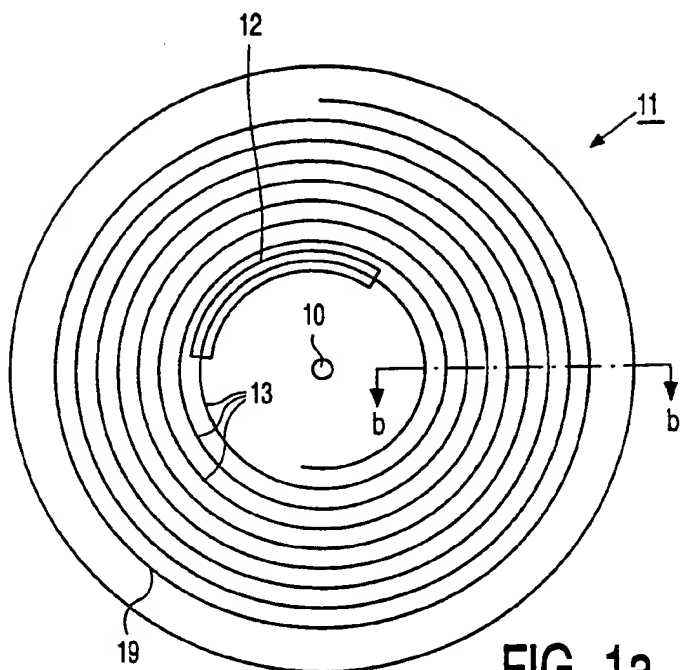


FIG. 1a

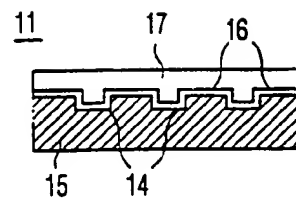


FIG. 1b

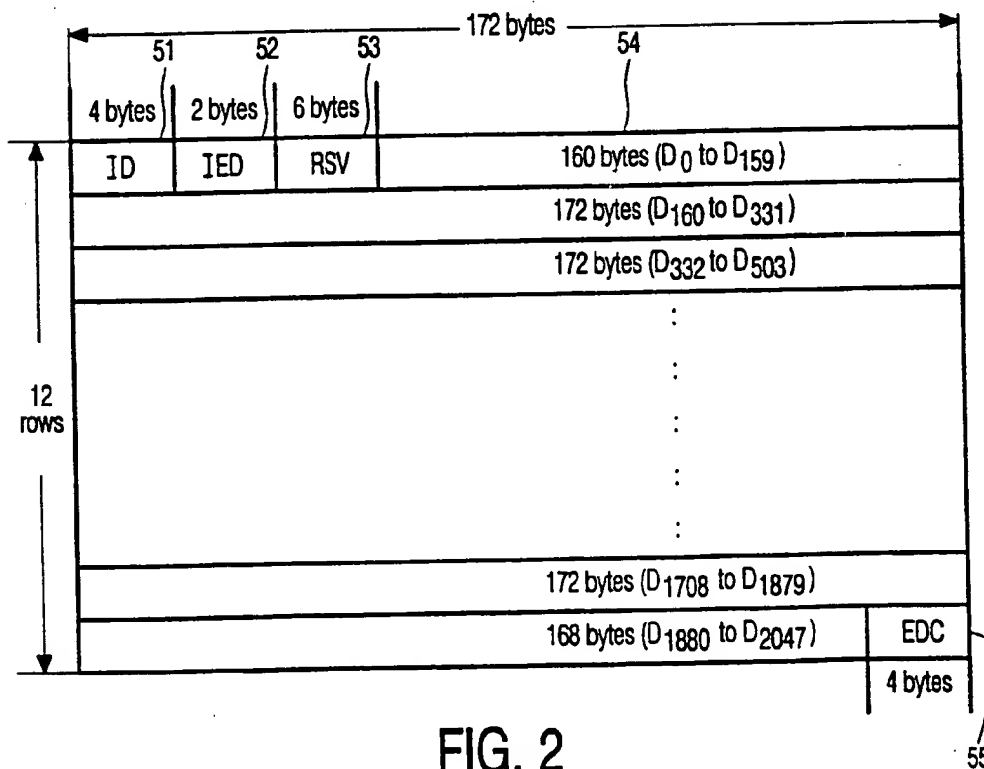


FIG. 2

2/5

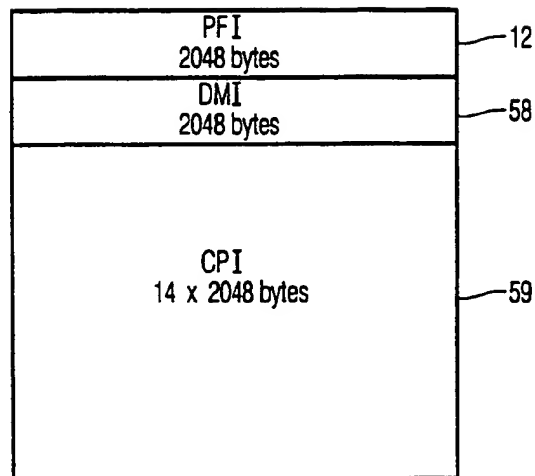


FIG. 3

Byte number	Content	Number of bytes
0	DCV	1
1	DSR	1
2	DS	1
3	RD	1
4 to 15	DZ	12
16	RSV	1
17 to 31	RSV	15
31 to 2047	RSV	2016

FIG. 4

Byte number	Content	Number of bytes
0 to 15	CON	16
16 to 2047	RSV	2032

FIG. 5

3/5

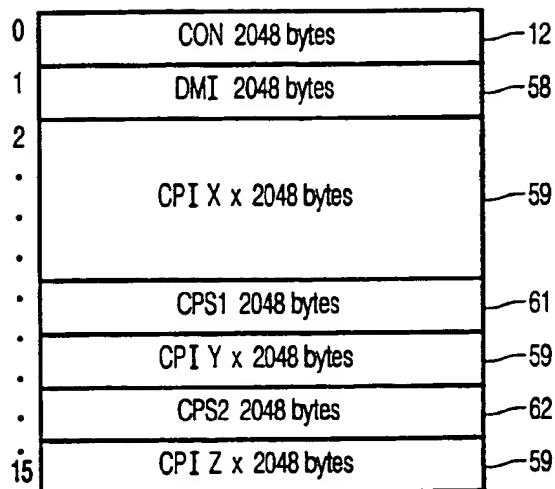


FIG. 6

Byte number	Content	Number of bytes
0 to 15	DFD	16
16 to 2047	RSV	2032

FIG. 7

Byte number	Content	Number of bytes
0 to m	DFK	m+1
m to n	E IV	n - m+1
n to 2047	RSV	2048 - n

FIG. 8

4/5

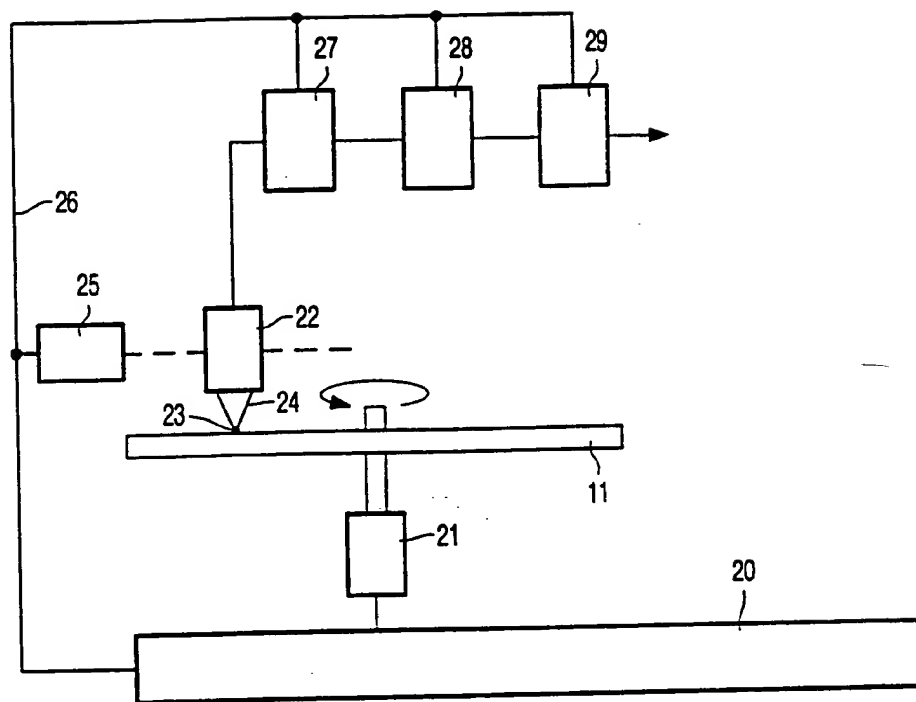


FIG. 9

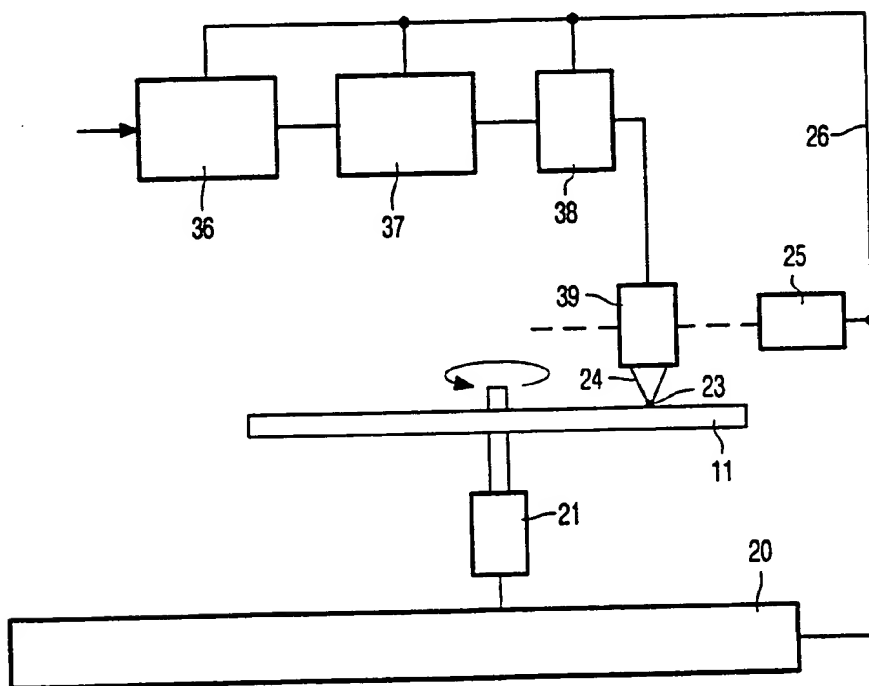


FIG. 10

5/5

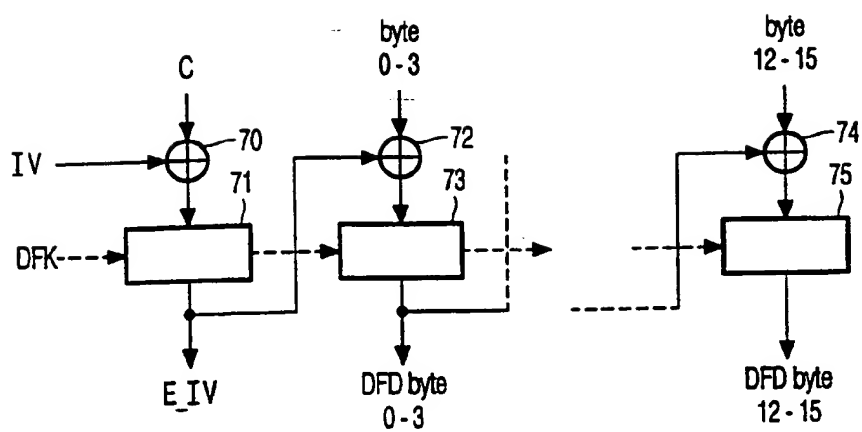


FIG. 11

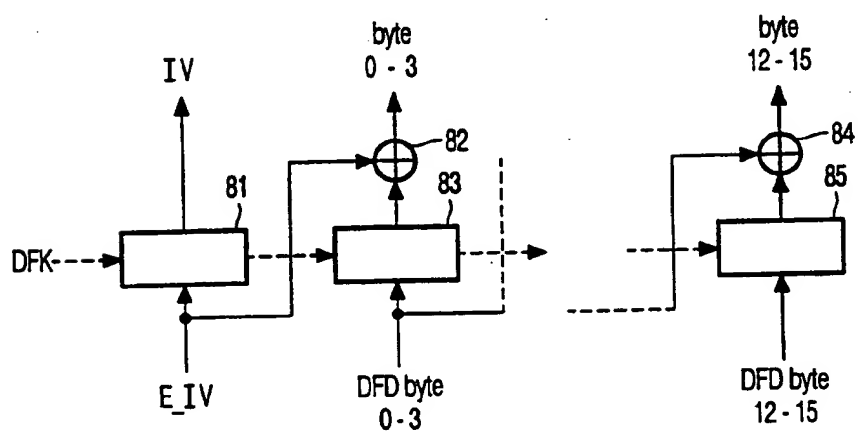


FIG. 12

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP 99/06789

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G11B20/12 G11B7/007

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 849 836 A (KACHIKIAN KEVIN R) 18 July 1989 (1989-07-18) column 1, line 40 -column 2, line 14 column 2, line 54 -column 3, line 9 column 3, line 57 -column 4, line 24 ---	1,12,13
A	US 5 644 444 A (BRAITHWAITE DAVID G ET AL) 1 July 1997 (1997-07-01) column 2, line 35 -column 3, line 40 column 5, line 8 -column 6, line 33 column 7, line 58 -column 8, line 51 ---	1,2,8,9,13
A	EP 0 342 748 A (PHILIPS NV) 23 November 1989 (1989-11-23) abstract column 6, line 34 -column 7, line 21 claim 1; figure 3 --- -/--	1

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

G document member of the same patent family

Date of the actual completion of the international search

29 December 1999

Date of mailing of the international search report

12/01/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Schiwy-Rausch, G

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 99/06789

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>PATENT ABSTRACTS OF JAPAN vol. 010, no. 389 (P-531), 26 December 1986 (1986-12-26) & JP 61 178732 A (MATSUSHITA ELECTRIC IND CO LTD), 11 August 1986 (1986-08-11) abstract</p> <p>-----</p>	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/06789

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 4849836	A	18-07-1989	NONE	
US 5644444	A	01-07-1997	CA 2211590 A DE 789908 T EP 0789908 A JP 10504420 T WO 9628820 A US 5949601 A	19-09-1996 19-02-1998 20-08-1997 28-04-1998 19-09-1996 07-09-1999
EP 0342748	A	23-11-1989	NL 8801275 A AT 101295 T AU 634709 B AU 3480589 A CA 1330591 A CN 1037790 A, B CZ 8902870 A DE 68912823 D DE 68912823 T ES 2050780 T HK 45796 A JP 2050360 A JP 2840631 B KR 148118 B SK 287089 A US 5418764 A US 5060219 A US 5654947 A	18-12-1989 15-02-1994 04-03-1993 23-11-1989 05-07-1994 06-12-1989 15-07-1998 17-03-1994 04-08-1994 01-06-1994 22-03-1996 20-02-1990 24-12-1998 15-10-1998 05-01-1995 23-05-1995 22-10-1991 05-08-1997
JP 61178732	A	11-08-1986	NONE	